Zero Trust Maturity Model

Pre-decisional Draft

June 2021

Version 1.0

Cybersecurity and Infrastructure Security Agency
Cybersecurity Division

Disclaimer

This document is designed to be a stopgap solution to support Federal Civilian Executive Branch (FCEB) agencies in designing their zero trust architecture (ZTA) implementation plans in accordance with Section 3,b,ii of Executive Order 14028, "*Improving the Nation's Cybersecurity*" . This document is a pre-decisional draft.

The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model is one of many paths to support the transition to zero trust.

Assumptions and Constraints

- This document is only meant to meet the specific task of assisting agencies with their zero trust migration plans. CISA will continue to publish zero trust guidance outside of this document.
- This document may be refined as zero trust evolves across the federal landscape.
- This document is not meant to be a robust set of guidance towards zero trust.
- This document reflects the seven tenants of zero trust as outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207.
    - All data sources and computing services are considered resources
    - All communication is secured regardless of network location.
    - Access to individual enterprise resources is granted on a per-session basis.
    - Access to resources is determined by dynamic policy.
    - The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
    - All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
    - The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.
- The path to zero trust is an incremental process that will take years to implement.
- Legacy infrastructure and systems may not support a zero trust implementation.

Zero Trust Maturity Model

Table of Contents

List of Figures

List of Tables

1. Introduction

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) provides support to agencies for evolving and operationalizing cybersecurity programs and capabilities. As the cyber risk advisor for .gov, CISA seeks to provide enhanced support for agencies adopting cloud services to improve situational awareness and incident response in cloud environments. To do this, CISA is re-examining legacy programs and capabilities while increasing its focus on operationalizing support for agencies. This document supports the continued evolution of CISA's programs and capabilities within a rapidly evolving environment and technology landscape by focusing on modernization efforts related to zero trust. This Zero Trust Maturity Model is one of many paths to support the transition to zero trust.

2. Environment

Recent cyber breaches have had wide-ranging implications and demand a federal response. Cyber defense requires greater speed and agility to outpace our adversaries, substantially increased costs and risks to threat actors, and the durability and resiliency to recover immediately. These compromises demonstrate that "business as usual" approaches are no longer acceptable for defending the nation from cyber threats, and new requirements hold CISA responsible for defending the.gov in clearer, more sophisticated and risk-informed ways.

CISA has a responsibility to maintain situational awareness and security for .gov. This responsibility makes CISA the risk advisor for federal civilian cybersecurity. CISA is responsible for aiding federal agencies, critical infrastructure, and industry partners as they defend against, respond to, and recover from major cyber incidents.

Executive Order 14028*, "Improving the Nation's Cybersecurity"* [1] marks a renewed commitment and prioritization of federal cybersecurity modernization and strategy. Among other policy mandates, the Executive Order (EO) embraces zero trust as the desired model for security and tasks CISA with modernizing its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with zero trust architecture (ZTA). While the EO marks a shift in federal policy, many efforts undertaken in recent years laid the foundation for the release of this EO.

Congress has also placed significant expectations on CISA by investing in improvements to the agency. The National Defense Authorization Act of 2020 and 2021 (NDAA)[2] expands CISA's authorities to hunt for threats, manage vulnerabilities, mitigate risk, and provide cybersecurity shared services for .gov. These investments enable CISA to create advanced cyber security and infrastructure security capabilities imperative to protecting and supporting .gov and critical infrastructure stakeholders.

3. Executive Order on Improving the Nation's Cybersecurity

The EO calls for Federal Civilian Executive Branch (FCEB) agencies to develop migration plans for ZTAs. A typical migration plan will assess an agency's current cybersecurity state and plan for a fully implemented ZTA. As the lead agency on federal cybersecurity and risk advisory, CISA's Zero Trust Maturity Model will assist agencies in the development of their Zero Trust strategies and implementation plans, and present ways in which various CISA services can support zero trust solutions across agencies.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[2] https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf

4. What Is Zero Trust?

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207 provides the following operative definition of zero trust and ZTA:

> **Zero trust** provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. **ZTA** is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.[3]

The publication goes on to emphasize that "the goal is to *prevent unauthorized access to data and services* coupled with making the *access control enforcement as granular as possible*." Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time; for these reasons, moving to a ZTA is non-trivial. This provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. More fundamentally, zero trust may require a change in an organization's philosophy and culture around cybersecurity. The path to zero trust is a journey that will take years to implement.

5. Other Federal Efforts on Zero Trust

The following publications on ZTAs in the Federal Government were consulted as CISA developed this guidance.

National Institute of Standards and Technology Special Publication 800-207
This document is intended to describe zero trust for enterprise security architects. It is meant to aid understanding of zero trust for civilian unclassified systems and provide a road map to migrate and deploy zero trust security concepts to an enterprise environment. This document is the product of a collaboration between multiple federal agencies and is overseen by the Federal Chief Information Officer (CIO) Council.

Department of Defense Zero Trust Reference Architecture
The scope of the Department of Defense (DOD) Zero Trust Reference Architecture[4] effort is specifically to determine capabilities and integrations that can be used to successfully advance the DOD Information Network (DODIN) into an interoperable zero trust end state. The architecture focused on data-centric design, while maintaining loose coupling across services to maximize interoperability. This document will evolve as requirements, technology, and best practices evolve and mature.

[3] NIST SP 800-207: Zero Trust Architecture. 2020.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[4] https://disa.mil/NewsandEvents/2021/ZeroTrust;
https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

National Security Agency Embracing Zero Trust Security Model
This document[5] explains the zero trust security model and its benefits, as well as challenges for implementation. It discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to the zero trust model to achieve the desired results. The document's recommendations will assist cybersecurity leaders, enterprise network owners, and administrators who are considering embracing this modern cybersecurity model.

6. Challenge

The Federal Government faces several challenges in transitioning to ZTA. First, legacy systems rely on "implicit trust"; this concept conflicts with the core principle of adaptive evaluation of trust within a ZTA. Additionally, existing infrastructures are also built on implicit trust and must either be rebuilt or replaced. To rebuild or replace information technology (IT) infrastructure and mission systems requires a significant investment on the part of agencies. Lastly, there is no consensus on or formal adoption of a maturity model for ZTA. While proposals for maturity models have been put forth, current initiatives for kickstarting zero trust adoption are often focused on the network layer and do not present a holistic approach for transition.

7. Current State and Future Vision

CISA provides security and situational awareness to agencies by providing guidance, executing strategy, developing and deploying architectures, and collecting telemetry. CISA programs seek to operationalize protections through its programs, such as:

- Continuous Diagnostics and Mitigation (CDM),
- Trusted Internet Connections (TIC),
- National Cybersecurity Protection System (NCPS),
- High Value Assets (HVA),
- Cyber Quality Service Management Office (QSMO) Marketplace, and
- Threat Hunting (TH).

Current capabilities defend against and mitigate known or suspected cyber threats. These capabilities, while necessary, are being challenged by the adoption of new and emerging technologies, as well as an evolving threat landscape.

The EO states that "CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with ZTA." Thus, CISA programs will evolve and new CISA programs may emerge to align with this EO.

Zero trust adoption will require engagement and cooperation of senior leadership, IT staff, and users across the Federal Government to effectively achieve design objectives and improve cybersecurity posture. This also includes current and future plans to adopt cloud technologies. This modernization of the Federal Government's cybersecurity will require agencies to transition stove-piped and siloed IT services and staff to coordinated and collaborative components of a zero trust strategy.

[5] https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/

The EO directs agencies to incorporate the steps NIST has outlined, listed below, in their migration plans.

Transitioning to Zero Trust:

1. Identify Actors on the Enterprise.
2. Identify Assets Owned by the Enterprise.
3. Identify Key Processes and Evaluate Risks Associated with Executing Process.
4. Formulating Policies for the ZTA Candidate.
5. Identifying Candidate Solutions.
6. Initial Deployment and Monitoring. [6]

8. Zero Trust Maturity Model

The Zero Trust Maturity Model represents a gradient of implementation across five distinct pillars, where minor advancements can be made over time toward optimization. The pillars, depicted in Figure 1, include Identity, Device, Network, Application Workload, and Data. Each pillar also includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance. **This maturity model is one of many paths to support the transition to zero trust.**

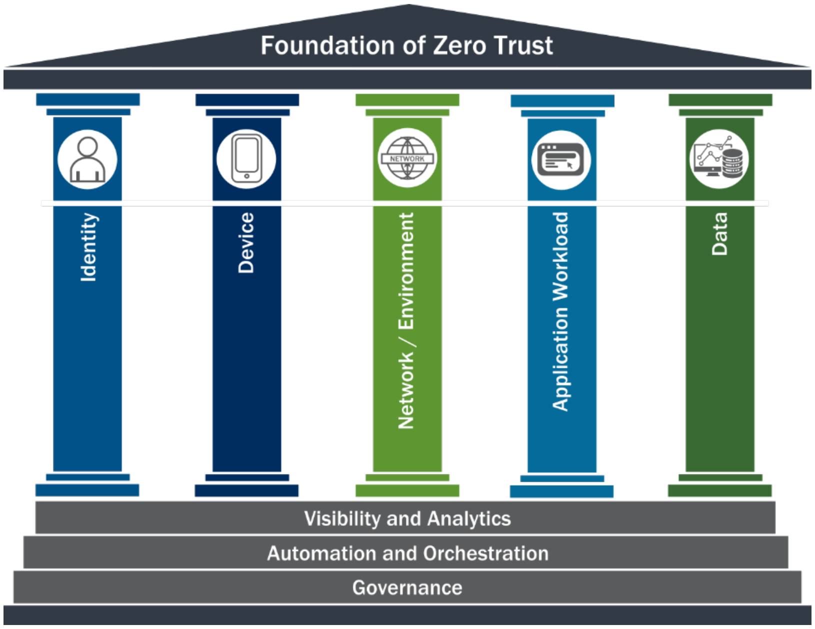


Figure 1: Foundation of Zero Trust[7]

As implementers transition towards optimal zero trust implementations, their solutions increase in reliance upon automated processes and systems, more fully integrate across pillars, and become more dynamic in their policy enforcement decisions. Each pillar can progress at its own pace and may be

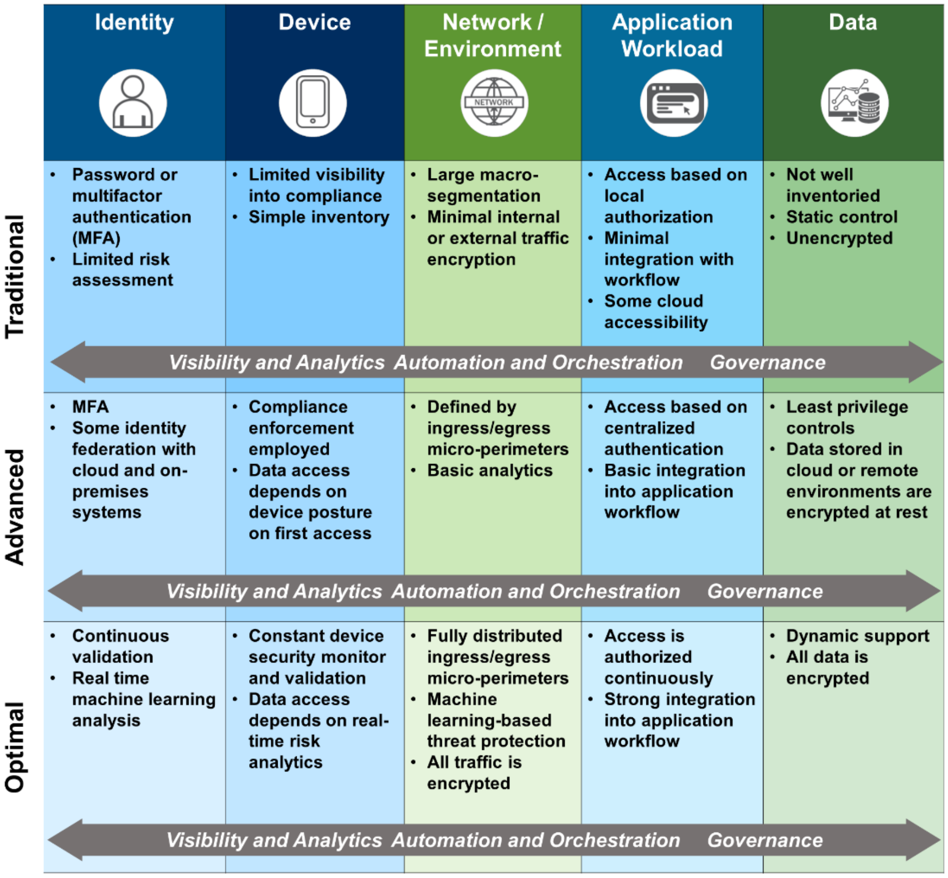
[6] NIST SP 800-207: Zero Trust Architecture. 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[7] This illustration was inspired by Figure 1 of the American Council for Technology (ACT) and Industry Advisory Council (IAC) "Zero Trust Cybersecurity Current Trends," (2019). https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

farther along than others, until cross-pillar coordination is required. Additionally, the interoperability and dependencies within the cross-pillar coordination must ensure compatibility. This allows for a gradual evolution to zero trust, distributing costs over time rather than entirely upfront. To facilitate migration, the Zero Trust Maturity Model gradient can be described using three stages, with increasing levels of protection, detail, and complexity for adoption, as outlined below. The following descriptions of each stage were used to identify maturity for each zero trust technology pillar and to provide consistency across the maturity model:

- **Traditional** – manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment.
- **Advanced** – some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments.
- **Optimal** – fully automated assigning of attributes to assets and resources, dynamic policies based on automated/observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with historian functionality for point-in-time recollection of state.

Figure 2 illustrates a high-level view of the Zero Trust Maturity Model across each maturity stage.



	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
	Visibility and Analytics Automation and Orchestration Governance				
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics Automation and Orchestration Governance				
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted
	Visibility and Analytics Automation and Orchestration Governance				

Figure 2: High-Level Zero Trust Maturity Model

These maturity stages, and the more specific details associated with each pillar below, can allow agencies to plan, assess, and maintain the investments needs to progress toward a ZTA. The following subsections provide high-level information to support agencies in transitioning to zero trust across the five different pillars: Identity, Device, Network, Application Workload, and Data. Each pillar also includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance for that pillar.

8.1 Pillar #1 Identity

An identity refers to an attribute or set of attributes that uniquely describe an agency user or entity. Agencies should ensure and enforce that the right users and entities have the right access to the right resources at the right time. Table 1 lists identity functions pertaining to zero trust and considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of identity.

Table 1: Identity Pillar

Function	Traditional	Advanced	Optimal
Authentication	Agency authenticates identity using either passwords or multi-factor authentication (MFA).	Agency authenticates identity using MFA.	Agency continuously validates identity, not just when access is initially granted.
Identity Stores	Agency only uses on-premises identity providers.	Agency federates some identity with cloud and on-premises systems.	Agency has global identity awareness across cloud and on-premises environments.
Risk Assessment	Agency makes limited determinations for identity risk.	Agency determines identity risk based on simple analytics and static rules.	Agency analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection.
Visibility and Analytics Capability	Agency segments user activity visibility with basic and static attributes.	Agency aggregates user activity visibility with basic attributes and then analyzes and reports for manual refinement.	Agency centralizes user visibility with high fidelity attributes and user and entity behavior analytics (UEBA).
Automation and Orchestration Capability	Agency manually administers and orchestrates (replicates) identity and credentials.	Agency uses basic automated orchestration to federate identity and permit administration across identity stores.	Agency fully orchestrates the identity lifecycle Dynamic user profiling, dynamic identity and group membership, just-in-time and just-enough access controls are implemented.
Governance Capability	Agency manually audits identities and permissions after initial provisioning using static technical enforcement of credential policies (e.g., complexity, reuse, length, clipping, MFA, etc.).	Agency uses policy-based automated access revocation. There are no shared accounts.	Agency fully automates technical enforcement of policies. Agency updates policies to reflect new orchestration options.

8.1.1 CISA Alignment to the Identity Pillar

Identity will form a core component of an agency's ZTA. Least privilege access, which underpins zero trust, depends on the ability to assure the identity of the entity receiving access. The Zero Trust Maturity Model moves away from simply using passwords to validate identity and instead uses a combination of factors to validate and continuously verify that identity throughout the duration of their interactions with services or data.

As agencies migrate services to the cloud, their users will have identities among a variety of providers. To effectively manage these identities and align security protections holistically, agencies will need to integrate their on-premises identities with those in the cloud environments. These integrated identities, however, can increase the attack surface of the agency because a compromised identity or identity provider may permit access across the broader agency environment.

Current CISA services and offerings:

- Capabilities to help agencies gain a better understanding of their users.

Tentative offerings that CISA will provide:

- Best practices for agencies looking to use multi-factor authentication to increase the security of identities.
- Expanded visibility that agencies can submit, including information around identity and access. This will enable CISA to provide better protections to help mitigate identity risks.

8.2 Pillar #2 Device

A device refers to any hardware asset that can connect to a network, including internet of things (IoT) devices, mobile phones, laptops, servers, and others. A device may be agency-owned or bring-your-own-device (BYOD). Agencies should inventory devices, secure all agency devices, and prevent unauthorized devices from accessing resources. Table 2 lists devices functions pertaining zero trust, as well as considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of devices.

Table 2: Device Pillar

Function	Traditional	Advanced	Optimal
Compliance Monitoring	Agency has limited visibility into device compliance.	Agency employs compliance enforcement mechanisms for most devices.	Agency constantly monitors and validates device security posture.
Data Access	Agency's access to data does not depend on visibility into the device that is being used to access the data.	Agency's access to data considers device posture on first-access.	Agency's access to data considers real-time risk analytics about devices.
Asset Management	Agency has a simplified and manually-tracked device inventory.	Agency uses automated methods to manage assets, identify vulnerabilities, and patch assets.	Agency integrates asset and vulnerability management across all agency environments, including cloud and remote.
Visibility and Analytics Capability	Agency's device management relies upon manual inspections of labels and periodic network discovery and reporting.	Agency reconciles device inventories against sanctioned lists with isolation of non-compliant components.	Agency continuously runs device posture assessments (e.g., using endpoint detection and response (EDR) tools).
Automation and Orchestration Capability	Agency manually provisions devices with static capacity allocations.	Agency provisions devices using automated, repeatable methods with policy-driven capacity allocations and reactive scaling.	Agency's device capacity and deployment uses continuous integration and continuous deployment (CI/CD) principles with dynamic scaling.
Governance Capability	Agency manually defines and enforces device acquisition channels and establishes and implements inventory frequency policy. Device retirement requires extensive sanitation to remove residual access and data.	Agency devices natively support modern security functions in hardware. Agency minimizes the quantity of legacy equipment that is unable to perform desired security functions.	Agency devices permit data access and use without resident plain-text copies, reducing asset supply chain risks.

8.2.1 CISA Alignment to the Device Pillar

The Zero Trust Maturity Model entails not just validating the identity of users, but also ensuring the integrity of the devices they use to access services and data. Agencies need to manage the security of these devices, ensuring a baseline of device security protections and visibility into the devices themselves.

The maturity model pushes policy enforcement to the edges, increasing the opportunities to make services and data available directly to users without routing through traditional access points. This endpoint focus allows for device compliance and integrity to be included as part of the access control decisions for services and data.

Current CISA services and offerings:

- Capabilities to understand the types of devices being used on their networks.
- Initial guidance and best practices to help agencies as they think through this migration towards the endpoints.

Tentative offerings that CISA will be providing:

- Capabilities that help ensure appropriate endpoint security.
- Capabilities that help provide agencies with security information about mobile applications to better ensure the security of the devices.
- Capabilities to protect endpoints while providing enhanced visibility to agencies.
- Additional guidance to help agencies better integrate device compliance into their access control and risk decisions.
- Enhanced endpoint visibility that agencies can provide to CISA, enabling CISA to provide better understand and protect agencies.

8.3 Pillar #3 Network/Environment

A network refers to an open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages. Agencies should segment and control networks and manage internal and external data flows. Table 3 lists networks/environments functions pertaining zero trust, as well as the considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of networks/environments.

Table 3: Network/Environment Pillar

Function	Traditional	Advanced	Optimal
Network Segmentation	Agency defines their network architecture using large perimeter/macro-segmentation.	Agency defines more of their network architecture by ingress/egress micro-perimeters with some internal micro-segmentation.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and deeper internal microsegmentation based around application workflows.
Threat Protection	Agency bases threat protections primarily on known threats and static traffic filtering.	Agency includes basic analytics to proactively discover threats.	Agency integrates machine learning-based threat protection and filtering with context-based signals.
Encryption	Agency explicitly encrypts minimal internal or external traffic.	Agency encrypts all traffic to internal applications, as well as some external traffic.	Agency encrypts all traffic to internal and external locations, where possible.
Visibility and Analytics Capability	Agency provides visibility at perimeter with centralized aggregation and analysis.	Agency integrates analysis across multiple sensor types and positions with manual policy-driven alerts and triggers.	Agency integrates analysis across multiple sensor types and positions with automated alerts and triggers.
Automation and Orchestration Capability	Agency manually initiates and executes network and environment changes following change management workflows.	Agency uses automated workflows to manually initiate network and environment changes.	Agency network and environment configurations use infrastructure-as-code, with pervasive automation, following (CI/CD) deployment models.
Governance Capability	Agency uses manual policies to identify sanctioned networks, devices, and services, with manual discovery and remediation of unauthorized entities.	Agency uses manual policies to identify sanctioned networks, devices, and services, with alerts and triggers and manual remediation for unauthorized entities.	Agency uses automated discovery of networks, devices, and services, with manual or dynamic authorization and automated remediation of unauthorized entities.

8.3.1 CISA Alignment to the Network/Environment Pillar

As agencies look to migrate toward a zero trust posture, they need to align their network segmentation and protections according to the needs of their application workflows instead of the implicit trust inherent in traditional network segmentation. This realignment in networking and protections can enable a rethinking of the traditional models of agency connectivity, enabling agencies to make applications and services available directly to remote users and branch offices. Through this migration process, agencies will need to consider the protections they deploy and where they can be deployed. Their existing protections may need to be augmented to ensure commensurate or improved protections in their rearchitected environment.

Current CISA services and offerings:

- Capabilities and guidance to help agencies gain a better understanding of their assets, users and data flows, and the protections that they may need to apply.
- Recent guidance on how to move away from perimeter-based protections, and how to align their protections in a more holistic manner.
- Visibility services to leverage more efficient operational architectures and cloud environments.

Tentative offerings that CISA will be providing:

- Expanded visibility offerings to enable CISA to better understand and protect agencies.
- Advanced protective domain name system (DNS) services.
- Matured offerings from shared security service providers.

8.4 Pillar #4 Application Workload

Applications and workloads include agency systems, computer programs, and services that execute on-premise, as well as in a cloud environment. Agencies should secure and manage the application layer as well as containers and provide secure application delivery. Table 4 lists application workload functions pertaining to zero trust, as well as the considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of application workload.

Table 4: Application Workload Pillar

Function	Traditional	Advanced	Optimal
Access Authorization	Agency's access to applications is primarily based on local authorization and static attributes.	Agency's access to applications relies on centralized authentication, authorization, monitoring, and attributes.	Agency continuously authorizes access to applications, considering real-time risk analytics.
Threat Protections	Agency threat protections have minimal integration with application workflows, applying general purpose protections for known threats.	Agency has basic integration of threat protections into application workflows, primarily applying protections for known threats with some application-specific protections.	Agency strongly integrates threat protections into application workflows, with analytics to provide protections that understand and account for application behavior.
Accessibility	Some critical cloud applications are directly accessible to users over the internet, with all others available through a virtual private network (VPN).	All cloud applications and some on-premises applications are directly accessible to users over the internet, with all others available through a VPN.	All applications are directly accessible to users over the internet.
Application Security	Agency performs application security testing prior to deployment, primarily through static and manual testing methods.	Agency integrates application security testing into the application development and deployment process, including the use of dynamic testing methods.	Agency integrates application security testing throughout the development and deployment process, with regular automated testing of deployed applications.
Visibility and Analytics Capability	Agency performs application health and security monitoring in isolation of external sensors and systems.	Agency performs application health and security monitoring in context with some external sensors and systems.	Agency performs continuous and dynamic application health and security monitoring with external sensors and systems.
Automation and Orchestration Capability	Agency establishes application hosting location and access at provisioning.	Applications can inform device and network components of changing state.	Applications adapt to ongoing environmental changes for security and performance optimization.

Function	Traditional	Advanced	Optimal
Governance Capability	Agency has legacy policies and conducts manual enforcement for software development, software asset management, security tests and evaluations (ST&E) at technology insertion, and tracking software dependencies.	Agency has updated policies and centralized enforcement.	Agency has updated policies and dynamic enforcement.

8.4.1 CISA Alignment to the Application Workload Pillar

To realign security protections based on zero trust principles, agencies will need to integrate their protections more closely with their application workflows to ensure the protections have the visibility and understanding needed to provide effective security. With access to applications based on identity, device compliance and other attributes, agencies may consider making these applications available to users directly. The enhanced accessibility of these applications can improve the usability and performance for end users while potentially increasing the agency threat surface.

As agencies build out their ZTA, they may extend that model beyond the application itself, and apply zero trust principles to the development and deployment of those applications. Continuous integration and continuous deployment models that integrate security testing and verification into each step of the process can help provide assurances about deployed applications. This methodology can be applied to the entire application lifecycle to include monitoring of the health and security, through both external and internal means, of deployed applications, including each component of an application's workflow.

Current CISA services and offerings:

- Assessments and regular security monitoring of externally accessible applications.
- Threat-based assessments of cyber capabilities.

Tentative offerings that CISA will be providing:

- Capabilities that better align with agency application deployments.
- Acceptance of application-level telemetry from agency applications that can enable CISA to effectively detect malicious activity as agencies move toward a zero trust posture.

8.5 Pillar #5 Data

Agency data should be protected on devices, in applications, and networks. Agencies should inventory, categorize, and label data, protect data at rest and in transit, and deploy mechanisms for detection data exfiltration. Table 5 lists data functions pertaining to zero trust, as well as the considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of data.

Table 5: Data Pillar

Function	Traditional	Advanced	Optimal
Inventory Management	Agency manually categorizes data and has poor data inventorying, leading to inconsistent categorization.	Agency primarily inventories data manually with some automated tracking. Agency performs data categorization using a combination of manual and static analysis methods.	Agency continuously inventories data with robust tagging and tracking. Agency augments categorization with machine learning models.
Access Determination	Agency governs access to data by using static access controls.	Agency governs access to data using least privilege controls that consider identity, device risk, and other attributes.	Agency's access to data is dynamic, supporting just-in-time and just-enough principles, and continual risk-based determinations.
Encryption	Agency primarily stores data in on-premises data stores and where they are unencrypted at rest.	Agency stores data in cloud or remote environments where they are encrypted at rest.	Agency encrypts all data at rest.
Visibility and Analytics Capability	Agency has limited data inventories that prevent useful visibility and analytics except possibly in specific circumstances.	Most of the agency's data are inventoried and can be accounted for since the last inventory update. Analytics are limited to plaintext data.	Agency's data are inventoried and can always be accounted for. Agency logs and analyzes all access events for suspicious behaviors. Agencies perform analytics on encrypted data.
Automation and Orchestration Capability	Agency lacks consistent categorization and labeling, which prevents automation and orchestration. Some data management tasks run automatically.	Agency runs scheduled audits that locate high-value data and analyze access controls. There is limited automatic orchestration to apply controls and ensure backups are in place.	Agency automatically enforces strict access controls for high-value data. All high-value data is backed up regardless of its storage location. Data inventories are automatically updated.
Governance Capability	Agency largely enforces data protection and handling policies through administrative controls. Data categorization and data access authorizations are largely defined by distributed decision making.	Agency enforces data protections through mostly technical and some administrative controls. Data categorization and data access authorizations are defined with a method that better integrates diverse data sources.	Agency automatically always enforces data protections required by policy. Data categorization and data access authorizations are defined using a fully unified approach that integrates data, independent of source.

8.5.1 CISA Alignment to the Data Pillar

As agencies migrate towards ZTAs, their mindsets must shift to a "data-centric" approach to cybersecurity. As a first step, agencies should begin to identify, categorize, and inventory data assets. CISA recommends that agencies prioritize deploying data protections for their most critical data assets (e.g., high value assets (HVAs)).

Current CISA services and offerings:

- Technical guidance documents that can assist agencies in implementing and maintaining robust data security controls.
- Capabilities in data protection management.
- Lessons learned from agency assessments and best practices to provide continuous feedback and to inform agencies on what critical data protections should be in place across an agency's IT enterprise.

Tentative offerings that CISA will be providing:

- Readiness surveys to gauge the maturity of the zero trust pillars at agencies. CISA will provide agencies with unique zero trust maturity feedback on these surveys, and agencies can use this feedback to identify gaps and to prioritize data protections.

9. CISA Resources

CISA programs provide cybersecurity support and guidance across the zero trust pillar areas, including the integration of the pillars into a ZTA. The following documents are useful resources for agencies migrating to zero trust. These resources will continue to be reviewed and refined as agencies develop ZTAs. In addition, new resources will be added to this collection over time.

Continuous Diagnostics and Mitigation
CDM guidance can be found on the CDM homepage.

High Value Assets
HVA guidance can be found on the HVA PMO | CISA homepage.

- High Value Asset Control Overlay, Version 2.0, January 2021
- High Value Asset Control Overlay FAQ, Version 1.0, January 2018
- Securing High Value Assets, July 2018
- CISA Insights: Securing High Value Assets, September 2019
- Binding Operational Directive 18-02, May 2018

National Cybersecurity Protection System
NCPS guidance can be found on the NCPS Guidance Repository page.

- National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture Volume 1: General Guidance, Version 1.2, July 2020
- National Cybersecurity Protection System (NCPS) Cloud Interface Reference Architecture Volume 2: Reporting Pattern Catalog DRAFT, Version 1.0, December 2020

Quality Service Management Office

- Quality Services Management Office Fact Sheet
- Centralized Mission Support Capabilities for the Federal Government (M-19-16), April 2019

Trusted Internet Connections
TIC guidance can be found on the TIC Guidance Repository page.

- Trusted Internet Connections 3.0 Program Guidebook, Version 1.0, July 2020
- Trusted Internet Connections 3.0 Reference Architecture, Version 1.0, July 2020
- Trusted Internet Connections 3.0 Security Capabilities Catalog, Version 1.1, April 2021
- Trusted Internet Connections 3.0 Traditional TIC Use Case, Version 1.0, April 2021
- Trusted Internet Connections 3.0 Branch Office Use Case, Version 1.0, April 2021
- Trusted Internet Connections 3.0 Remote User TIC Use Case DRAFT, Version 1.0, December 2020

Other CISA Resources

- govCAR Recommendations: Mobile Cybersecurity
- Cyber Resilience Review Assessments
- govCAR Factsheet